manuscripta math.

Clemens Fuchs · Christina Karolus · Dijana Kreso

Decomposable polynomials in second order linear recurrence sequences

Received: 21 July 2017 / Accepted: 24 September 2018

Abstract. We study elements of second order linear recurrence sequences $(G_n)_{n=0}^{\infty}$ of polynomials in $\mathbb{C}[x]$ which are decomposable, i.e. representable as $G_n = g \circ h$ for some $g, h \in \mathbb{C}[x]$ satisfying $\deg g, \deg h > 1$. Under certain assumptions, and provided that h is not of particular type, we show that $\deg g$ may be bounded by a constant independent of n, depending only on the sequence.

1. Introduction and results

Let $d \geq 2$ be an integer. We consider a sequence of polynomials $(G_n)_{n=0}^{\infty}$ in $\mathbb{C}[x]$ satisfying the d-th order linear recurrence relation

$$G_{n+d}(x) = A_{d-1}(x)G_{n+d-1}(x) + \cdots + A_0(x)G_n(x), \quad n \in \mathbb{N}, \tag{1}$$

determined by $A_0, A_1, \ldots, A_{d-1} \in \mathbb{C}[x]$ and initial terms $G_0, G_1, \ldots, G_{d-1} \in \mathbb{C}[x]$. Let $\mathcal{G} \in \mathbb{C}(x)[T]$ be the characteristic polynomial of the sequence and let $\alpha_1, \ldots, \alpha_t$ be its distinct roots in the splitting field $L/\mathbb{C}(x)$ of $\mathcal{G}$, that is

$$\mathcal{G}(T) = T^d - A_{d-1}T^{d-1} - \cdots - A_0 = (T-\alpha_1)^{k_1}(T-\alpha_2)^{k_2}\cdots(T-\alpha_t)^{k_t},$$

where $k_1, \ldots, k_t \in \mathbb{N}$. Then G_n admits a representation of the form

$$G_n(x) = \pi_1\alpha_1^n + \pi_2\alpha_2^n + \cdots + \pi_d\alpha_d^n, \tag{2}$$

where $\pi_i \in L[n]$ for $i = 1, 2, \ldots, n$. We say that the recurrence relation (1) is *minimal* if $(G_n)_{n=0}^{\infty}$ does not satisfy a recurrence relation with smaller d and coefficients in $\mathbb{C}[x]$. We say that (1) is *non-degenerate* if $\alpha_i/\alpha_j \notin \mathbb{C}^*$ for all $i \neq j$. Finally, we say that (1) is *simple* if $k_1 = \cdots = k_t = 1$; in this case the π_i's lie in L. We also call the corresponding sequence $(G_n)_{n=0}^{\infty}$ minimal, non-degenerate and simple, respectively. In this paper, we will be concerned with second-order minimal non-degenerate simple linear recurrences.

C. Fuchs (✉) · C. Karolus: University of Salzburg, Hellbrunnerstr. 34/I, 5020 Salzburg, Austria. e-mail: clemens.fuchs@sbg.ac.at
C. Karolus: e-mail: christina.karolus@sbg.ac.at
D. Kreso: Graz University of Technology, Kopernikusgasse 24/II, 8010 Graz, Austria. e-mail: kreso@math.tugraz.at

Mathematics Subject Classification: 11B37 · 11R09 · 12E99 · 39B12

https://doi.org/10.1007/s00229-018-1070-8
Published online: 04 October 2018

Many Diophantine problems involving linear recurrence sequences have been studied in the literature. For example, a famous problem is to estimate the number of zeros appearing in such a sequence, and more generally, to bound the number of solutions $n \in \mathbb{N}$ of the equation $G_n(x) = a$, where $a \in L$ is given (cf. [9] and the papers cited therein). Also, several authors studied the problem of giving bounds on m and n such that $G_n(x) = cG_m(P(x))$, $c = c(n, m)$, where $(G_n)_{n=0}^{\infty}$ is a linear recurrence sequence and P a fixed polynomial (cf. [8,10–12]).

In this paper, we focus on *decomposable* polynomials in second order linear recurrence sequences. A polynomial $f \in \mathbb{C}[x]$ with $\deg f > 1$ is said to be decomposable if it can be written as the composition $f(x) = g(h(x))$ with $g, h \in \mathbb{C}[x]$ and $\deg g, \deg h > 1$, and *indecomposable* otherwise. The possible ways of writing a polynomial as a composition of polynomials were studied by several authors, starting with Ritt in the 1920's in his classical paper [21]. Results in this area of mathematics have applications to various other fields, e.g. number theory, complex analysis, arithmetic dynamics, finite geometries, etc. For example, there are applications to Diophantine equations of type $f(x) = g(y)$. In 2000, Bilu and Tichy [4], by building on the work of Siegel, Ritt, Fried and Schinzel, classified the polynomials f, g for which the equation $f(x) = g(y)$ has infinitely many solutions in S-integers x, y. It turns out that such f and g must be representable as a composition of polynomials in a certain prescribed way.

In this paper we show that if $(G_n)_{n=0}^{\infty}$ satisfies (1) with $d = 2$, under certain assumptions on G_0, G_1, A_0 and A_1, if $G_n(x) = g(h(x))$ and $h(x)$ is not of particular type, then $\deg g$ may be bounded by a constant independent of n, depending only on the sequence (more precisely, it depends only on the degrees of G_0, G_1, A_0, A_1). To describe what we mean by h being of particular type and to state our results, we introduce the following notions. We say that $f, g \in \mathbb{C}[x]$ are *equivalent* if there are linear $\ell_1, \ell_2 \in \mathbb{C}[x]$ such that $f(x) = \ell_1(x) \circ g(x) \circ \ell_2(x)$. For $f \in \mathbb{C}[x]$, we say that f is *cyclic* if it is equivalent to a polynomial g with $g(x) = x^n$ for some $n > 1$, and we say that f is *dihedral* if it is equivalent to T_n for some $n > 2$, where T_n is a Chebychev polynomial, defined by the functional equation $T_n(x + 1/x) = x^n + 1/x^n$. Cyclic and dihedral polynomials play an important role in Ritt's theory of polynomial decomposition, as will be explained in Sect. 2.

To see that at least some exceptional cases have to be taken into account, consider e.g. the well-known family of Fibonacci polynomials F_n, defined by

$$F_0(x) = 0, \quad F_1(x) = 1, \quad F_{n+2}(x) = xF_{n+1}(x) + F_n(x) \text{ for } n \in \mathbb{N}. \tag{3}$$

It is easy to see that for all odd $n \geq 3$, F_n is an even polynomial of degree $n - 1$, and hence if $n \geq 5$ is odd, $F_n(x)$ can be written as $F_n(x) = g(h(x))$, where $h(x) = x^2$ and $\deg g = (n-1)/2$. Clearly, here the degree of g cannot be bounded independently of n. In this case, h is cyclic.

Also, for Chebyshev polynomials T_n, which satisfy the second order linear recurrence

$$T_0(x) = 1, \quad T_1(x) = x, \quad T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x) \text{ for } n \in \mathbb{N},$$

it is well-known that $T_{mn} = T_m \circ T_n$ for any $m, n \in \mathbb{N}$. Since $\deg T_n = n$, clearly one cannot bound $\deg g$ independently of n assuming $T_n(x) = g(h(x))$ and $\deg h > 1$. In this case, h is dihedral.

There is a third, trivial situation where it is clearly not possible to bound the degree of g independently of n assuming $G_n = g \circ h$, namely when $G_m(x) \in \mathbb{C}[h(x)]$ for every $m \in \mathbb{N}$. Consider for example the sequence $(F_n(h(x)))_{n=0}^{\infty}$, where F_n is defined by (3) and $h \in \mathbb{C}[x]$. This sequence satisfies a second order linear recurrence relation and we clearly cannot bound $\deg F_n$ independently of n. It will be shown later that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$ if and only if $G_0, G_1, A_0, A_1 \in \mathbb{C}[h(x)]$, see Lemma 8.

We now describe our strategy and results in detail. Let $(G_n)_{n=0}^{\infty}$ be a minimal non-degenerate simple second order linear recurrence sequence given by (1) (with $d = 2$). Assume that G_n is decomposable for some $n \in \mathbb{N}$ and write $G_n(x) = g(h(x))$, where h is indecomposable, and thus $\deg h \geq 2$. By Gauss's lemma it follows that the polynomial $h(X) - h(x) \in \mathbb{C}(h(x))[X]$ is irreducible and since $h'(X) \neq 0$, it is also separable (find details in Sect. 2). Since $\deg h \geq 2$, there exists a root $y \neq x$ in its splitting field over $\mathbb{C}(h(x))$. Clearly, $h(x) = h(y)$. As in (2), we have

$$G_n(x) = \pi_1 \alpha_1^n + \pi_2 \alpha_2^n,$$

where α_1, α_2 are distinct roots of the characteristic polynomial $\mathcal{G}_1(T) = T^2 - A_1(x)T - A_0(x)$ in its splitting field $L_1/\mathbb{C}(x)$, and $\pi_1, \pi_2 \in L_1$. Indeed, there is a representation of this form since by assumption the characteristic polynomial has no multiple roots. Observe that $\pi_i \alpha_i^n \neq 0$ for all $n \in \mathbb{N}$ and $i = 1, 2$ by minimality. Conjugating (in some fixed algebraic closure of $\mathbb{C}(x)$ containing α_1, α_2) over $\mathbb{C}(h(x))$ via $x \mapsto y$, we get a sequence $(G_n(y))_{n=0}^{\infty}$ with $G_n(y) \in \mathbb{C}[y]$, which satisfies the same minimal non-degenerate simple recurrence relation as $(G_n(x))_{n=0}^{\infty}$ with x replaced by y. We conclude that

$$G_n(y) = \rho_1 \beta_1^n + \rho_2 \beta_2^n,$$

where β_1, β_2 are distinct roots of the characteristic polynomial $\mathcal{G}_2(T) = T^2 - A_1(y)T^{d-1} - A_0(y)$ in its splitting field $L_2/\mathbb{C}(y)$, and $\rho_1, \rho_2 \in L_2$. Again we have that $\rho_i \beta_i^n \neq 0$ for all $n \in \mathbb{N}$ and $i = 1, 2$. Since $h(x) = h(y)$, we get $G_n(x) = G_n(y)$, that is

$$\pi_1 \alpha_1^n + \pi_2 \alpha_2^n = \rho_1 \beta_1^n + \rho_2 \beta_2^n. \tag{4}$$

We view this last equation as an S-unit equation in function fields and seek to apply a result of Brownawell and Masser (see Theorem 3 below) to bound the height of G_n and consequently the degree of g. However, this theorem can be applied directly only to equations in which no proper subsum vanishes. We will show in Sect. 4 that if h is not cyclic, then equation (4) has a proper vanishing subsum if and only if

$$\pi_1 \pi_2 A_0(x)^n \in \mathbb{C}(h(x)).$$

In particular, the existence of a proper vanishing subsum of (4) does not depend on the choice of the conjugate y of x over $\mathbb{C}(h(x))$. However, (4) cleary depends

on n and h for which $G_n(x) = g(h(x))$ which are not known a priori. Note that if h is not cyclic and $A_0(x) = a_0 \in \mathbb{C}$, $\pi_1\pi_2 = \pi \in \mathbb{C}$, then there exists a vanishing subsum of (4) and one cannot apply the theorem in question; for example, this is the case for Chebyshev polynomials T_n.

We now state our main result.

Theorem 1. *Let $A_0, A_1, G_0, G_1 \in \mathbb{C}[x]$ and $(G_n)_{n=0}^{\infty}$ be a sequence of polynomials defined by the minimal non-degenerate simple linear recurrence*

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x), \quad n \in \mathbb{N}. \tag{5}$$

There is a positive real constant $C = C(\{A_i, G_i : i = 1, 2\})$ with the following property. If for some n we have $G_n(x) = g(h(x))$, where h is indecomposable and neither dihedral nor cyclic, and if (4) has no proper vanishing subsum, then it holds that $\deg g \leq C$.

We mention that the constant C in Theorem 1 can be effectively computed; this is done in the proof of the theorem. Since the bound is not very illuminating, we have not stated it above. Also note that in the theorem the situation that $G_m(x) \in \mathbb{C}[h(x)]$ for all m is not excluded explicitly. It will be shown (see Lemma 9) that in this case either h is cyclic or equation (4) has a proper vanishing subsum.

Theorem 1 resembles a result of Zannier [26], who showed that if f is a polynomial with ℓ non-constant terms and $f(x) = g(h(x))$, where h is not of type $ax^k + b$, $a \neq 0$, then $\deg g \leq 2\ell(\ell - 1)$. Our proof, like Zannier's proof, involves applying Brownawell and Masser's theorem [5]. The application of this theorem in our proof requires a different approach and the technical details are more challenging. We remark that Zannier's result was one of the main ingredients of the proof of a conjecture of Schinzel [27] by the same author, which states that for $f \in \mathbb{C}[x]$ with ℓ non-constant terms, satisfying $f = g \circ h$ for some $g, h \in \mathbb{C}[x]$, the number of terms of h is bounded above by $B(\ell)$, where B is an explicitly computable function. Zannier's result was then used in [15,16] to study Diophantine equations of type $f(x) = g(y)$, where f and g are arbitrary polynomials with a fixed number of non-constant terms, via the criterion of Bilu and Tichy. We remark that likewise, using our results, one may study Diophantine equations of this type where f and/or g are elements of a second order linear recurrence sequence of polynomials. We further mention that some special cases of the latter problem have already been studied in the literature, see [6,14].

In order to apply Theorem 1 one has to exclude that (4) has a proper vanishing subsum. This depends on n and h which are not known a priori. One therefore has to show that for all $n \in \mathbb{N}$ and for all $h \in \mathbb{C}[x]$, $\deg h > 1$, h not cyclic we have that $\pi_1\pi_2 A_0(x)^n \notin \mathbb{C}(h(x))$ holds. Verification of this turns out to be quite non-trivial and one might suspect that it is not possible to verify it at all. We therefore complement Theorem 1 by detecting some explicit cases for which there does not exist such a vanishing subsum with the motivation to convince the reader that Theorem 1 contains useful information and is applicable. In fact we believe that no vanishing subsum exists at all unless we are in one of the exceptional cases already mentioned in the theorem. It would be very interesting to see a proof or a counterexample of this.

To detect cases when there does not exist a vanishing subsum of (4), we apply several tools. We follow a Galois-theoretic approach to decomposition questions, which originated in Ritt's work [21], and apply some recent results on polynomial decomposition from [1] and [20]. We show that the following holds.

Theorem 2. *Let $A_0, A_1, G_0, G_1 \in \mathbb{C}[x]$ and $(G_n)_{n=0}^{\infty}$ be a sequence of polynomials defined by the minimal non-degenerate simple linear recurrence*

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x), \quad n \in \mathbb{N}.$$

Assume that for some n we have $G_n(x) = g(h(x))$, where h is indecomposable. If h is neither dihedral nor cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$, then (4) has no proper vanishing subsum if $A_0(x)$ is constant and any of the following holds:

i) $2G_1(x) = G_0(x)A_1(x)$, i.e. $\pi_1 = \pi_2$,
ii) $G_1(x) = 2A_0(x) + G_0(x)^2$, $G_0(x) = A_1(x)$,
iii) $G_1(x) = -2A_0(x)$, $G_0(x) = A_1(x)$.

If h is not cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$, then (4) has no proper vanishing subsum if any of the following holds:

i) $\pi_1\pi_2 = \pi A_0(x)^m$, *for some* $\pi \in \mathbb{C}$, $m \geq 0$ *and* $\deg A_0 = 1$,
ii) $\pi_1 = \pi_2 = \pi \in \mathbb{C}$ *and either* $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ *or* $\deg A_0 = 1$,
iii) $G_1(x) = 2A_0(x) + G_0(x)^2$, $G_0(x) = A_1(x)$ *and either* $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ *or* $\deg A_0 = 1$,
iv) $G_1(x) = -2A_0(x)$, $G_0(x) = A_1(x)$ *and either* $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ *or* $\deg A_0 = 1$.

We mention that the condition $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ means that the roots α_1, α_2 of the corresponding characteristic polynomial are in $\mathbb{C}[x]$. As clarified in the theorem, the condition $2G_1(x) = G_0(x)A_1(x)$ is equivalent to the condition $\pi_1 = \pi_2$. Furthermore, we mention that if $G_0(x) = A_1(x)$, and either $G_1(x) = 2A_0(x) + G_0(x)^2$ or $G_1(x) = -2A_0(x)$, then either $\pi_1 = \alpha_1$ and $\pi_2 = \alpha_2$, or $\pi_1 = \alpha_2$ and $\pi_2 = \alpha_1$ (see Lemma 10 and Lemma 11 for more details).

The paper is organized as follows. In Sect. 2 we shall collect some facts about polynomial decomposition; here Galois-theoretic arguments play an important role. In Sect. 3 we collect auxiliary results concerning heights in function fields, state some well-known theorems from the literature, and prove three lemmas which will be used to prove our main results. In Sect. 4 we give a proof of Theorem 2 using results from the previous two sections. In Sect. 5 we give a proof of Theorem 1. As already mentioned above, our proof of Theorem 1 involves applying the theory of S-unit equations over function fields.

2. Polynomial decomposition via Galois theory

Recall that a polynomial $f \in \mathbb{C}[x]$ with $\deg f > 1$ is called *indecomposable* if it cannot be written as the composition $f(x) = g(h(x))$ with $g, h \in \mathbb{C}[x]$, $\deg g > 1$

and $\deg h > 1$. Otherwise, f is said to be *decomposable*. Any representation of f as a functional composition of polynomials of degree > 1 is said to be a *decomposition* of f. A decomposition $f = f_1 \circ f_2 \circ \cdots \circ f_m$ of f is said to be *complete* if each f_i is an indecomposable polynomial.

Note that if $\mu \in \mathbb{C}[x]$ is linear, then there exists $\mu^{\langle -1 \rangle} \in \mathbb{C}[x]$ such that $(\mu \circ \mu^{\langle -1 \rangle})(x) = (\mu^{\langle -1 \rangle} \circ \mu)(x) = x$. Thus, $g \circ h = g \circ \mu \circ \mu^{\langle -1 \rangle} \circ h$. By comparison of degrees one sees that no such polynomial exists when $\deg \mu > 1$.

Definition 1. *Given $f \in \mathbb{C}[X]$ with* $\deg f > 1$*, the* monodromy group $\mathrm{Mon}(f)$ *of f is the Galois group of $f(X) - t$ over the field $\mathbb{C}(t)$, where t is transcendental, viewed as a group of permutations of the roots of $f(X) - t$.*

A lot of information about the polynomial f is encoded into its monodromy group. By Gauss's lemma it follows that $f(X) - t$ is irreducible over $\mathbb{C}(t)$, so $\mathrm{Mon}(f)$ is a transitive permutation group. Since $f'(X) \neq 0$, it follows that $f(X) - t$ is also separable. Let x be a root of $f(X) - t$ in its splitting field L over $\mathbb{C}(t)$. Then $t = f(x)$ and $\mathrm{Mon}(f) = \mathrm{Gal}(L/\mathbb{C}(f(x)))$ is viewed as a permutation group on the conjugates of x over $\mathbb{C}(f(x))$.

Lüroth's theorem (see [22, p. 13]) states that for a field K satisfying $\mathbb{C} \subset K \subseteq \mathbb{C}(x)$ we have $K = \mathbb{C}(h(x))$ for some $h \in \mathbb{C}(x)$. This theorem provides a dictionary between decompositions of $f \in \mathbb{C}[x]$ and fields between $\mathbb{C}(f(x))$ and $\mathbb{C}(x)$. Namely, if $f(x) = g(h(x))$, then $\mathbb{C}(f(x)) \subseteq \mathbb{C}(h(x)) \subseteq \mathbb{C}(x)$. On the other hand, if K is a field between $\mathbb{C}(f(x))$ and $\mathbb{C}(x)$, by Lüroth's theorem it follows that $K = \mathbb{C}(h(x))$ for some $h \in \mathbb{C}(x)$. Since f is a polynomial, h can be chosen to be a polynomial by [22, p. 16]. Then $f = g(h(x))$ for some $g \in \mathbb{C}[x]$. The fields between $\mathbb{C}(f(x))$ and $\mathbb{C}(x)$ clearly correspond to groups between the two associated Galois groups – $\mathrm{Gal}(L/\mathbb{C}(f(x))) = \mathrm{Mon}(f) =: G$ and $\mathrm{Gal}(L/\mathbb{C}(x)) =: H$ (the stabilizer of x in $\mathrm{Mon}(f)$). In this way, the study of ways to represent a polynomial f as a composition of lower degree polynomials reduces to a study of subgroups of the monodromy group of f, and more precisely to the study of groups between H and G. Furthermore, it can be shown that G has a transitive cyclic subgroup, that is that $G = HI$ for some cyclic group I (I can be chosen to be the inertia group at any place of the splitting field of $f(x) - t$ which lies over the infinite place of $\mathbb{C}(t)$); see also [17, Lemma 3.4] or [24, Lemma 3.3]. In this way, the study of ways to represent a complex polynomial f as a composition of lower degree polynomials reduces to a study of subgroups of the cyclic group I.

The interested reader is referred to [17] and [20] to find out more about the Galois-theoretic setup for addressing decomposition questions which originated in Ritt's work [21]. Ritt in [21] also showed that any complete decomposition of a complex polynomial f can be obtained from any other through a sequence of steps, each of which involves replacing two adjacent indecomposables by two others with the same composition. He then solved the equation $a \circ b = c \circ d$ in indecomposable complex polynomials, showing that the only solutions, up to composing with linear polynomials, are the trivial one $a \circ b = a \circ b$ and the non-trivial solutions

$$x^n \circ x^k h(x^n) = x^k h(x)^n \circ x^n \quad \text{and} \quad T_m(x) \circ T_n(x) = T_n(x) \circ T_m(x),$$

where $h \in \mathbb{C}[x]$, $n, k, m \in \mathbb{N}$ and T_n is the n-th Chebyshew polynomial defined in the introduction. We now record two results on the topic that we will repeatedly use in the sequel.

Proposition 1. *Pick $f \in \mathbb{C}[x]$ of degree $\deg f > 1$. For any two complete decompositions $f = f_1 \circ f_2 \circ \cdots \circ f_m = g_1 \circ g_2 \circ \cdots \circ g_n$ of f, we have that $m = n$ and $\mathrm{Mon}(f_i) \cong \mathrm{Mon}(g_{\sigma(i)})$ for some permutation σ of the set $\{1, 2, \ldots, m\}$ and for all $i = 1, 2, \ldots, m$.*

Proposition 2. *Pick $f \in \mathbb{C}[x]$ of degree $n > 1$. Then $\mathrm{Mon}(f)$ is cyclic if and only if f is cyclic, in which case $|\mathrm{Mon}(f)| = n$. Likewise, if $n > 2$, then $\mathrm{Mon}(f)$ is dihedral if and only if f is dihedral, in which case $|\mathrm{Mon}(f)| = 2n$.*

Recall that for $f \in \mathbb{C}[x]$, we say that f is cyclic if it is equivalent to x^n for some $n > 1$, and we say that f is dihedral if it is equivalent to T_n for some $n > 2$. Proposition 1 is Theorem 1.3 in [20]. See also [17, Thm. 5.1]. Proposition 2 is Lemma 3.6 in [20]. See also Theorem 3.8 in [3]. We record the following corollary.

Lemma 1. *Pick $f \in \mathbb{C}[x]$ with $\deg f > 1$. If f is dihedral, then for any complete decomposition of f the collection of monodromy groups of the indecomposable polynomials consists only of dihedral groups. Furthermore, if f is cyclic, then for any complete decomposition of f the collection of monodromy groups of the indecomposable polynomials consists only of cyclic groups.*

Proof. By Proposition 2, it suffices to prove the statement in the cases $f(x) = T_m(x)$ and $f(x) = x^m$ for $m \in \mathbb{N}$, respectively. Note that since $T_{mn}(x) = T_m(T_n(x))$ for any $m, n \in \mathbb{N}$ and $\mathrm{Mon}(f)$ is dihedral if and only if f is dihedral, for any $m \in \mathbb{N}$ there exists a complete decomposition of $T_m(x)$ such that the collection of monodromy groups of the indecomposable polynomials consists only of dihedral groups. By Proposition 1, for any complete decomposition of $T_m(x)$ the collection of monodromy groups of the indecomposable polynomials consists only of dihedral groups. By the same argument, for any complete decomposition of x^m the collection of monodromy groups of the indecomposable polynomials consists only of cyclic groups. □

In the literature, quite often Ritt's and related results are expressed in terms of Dickson polynomials $D_n(x, a)$ (with parameter a), as they satisfy

$$D_n(2ax, a^2) = 2a^n T_n(x), \ a \neq 0, \quad D_n(x, 0) = x^n. \tag{6}$$

We refer to Turnwald's paper [24] for various properties of Chebyshev and Dickson polynomials. We now list some that will be of importance to us in this paper.

Proposition 3. *All of the following holds:*

- $T_0(x) = 1$, $T_1(x) = x$, $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, $n \geq 2$.
- $D_0(x, a) = 2$, $D_1(x, a) = x$, $D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a)$, $n \geq 2$.
- $T_{mn}(x) = T_m(T_n(x))$ *for any* $m, n \in \mathbb{N}$.
- $D_{mn}(x, a) = D_m(D_n(x, a), a^n)$ *for any* $m, n \in \mathbb{N}$.

- $D_n(x, 0) = x^n$.
- $D_n(x + a/x, a) = x^n + (a/x)^n$.
- $D_n(x + y, xy) = x^n + y^n$.
- *Let $n \geq 2$ and let $\zeta_n \in \mathbb{C}$ be a primitive n-th root of unity. Put $\gamma_k = \zeta_n^k + \zeta_n^{-k}$ and $\delta_k = \zeta_n^k - \zeta_n^{-k}$ (so that $\gamma_k^2 - 4 = \delta_k^2$). Then*

$$D_n(x, a) - D_n(y, a) = (x - y) \prod_{k=1}^{(n-1)/2} \left(x^2 - \gamma_k xy + y^2 + \delta_k^2 a\right),$$

when n is odd and

$$D_n(x, a) - D_n(y, a) = (x - y)(x + y) \prod_{k=1}^{(n-2)/2} \left(x^2 - \gamma_k xy + y^2 + \delta_k^2 a\right),$$

when n is even.

For the proof of Theorem 2 we will also need the following result about polynomials with a common composite, which can be deduced from a result of Beals, Wetherell and Zieve [1, Thm. 5.1]. If $f_1, f_2 \in \mathbb{C}[x]$ are non-constant polynomials for which there exist non-constant $u, v \in \mathbb{C}[x]$ such that $u(f_1(x)) = v(f_2(x))$, then f_1 and f_2 are said to have a *common composite*. 'Most' pairs of complex polynomials have no common composite (this follows to the most part already from Ritt's results, see [1] for the details). The following fact will be repeatedly used in our proof of Theorem 2.

Proposition 4. *Suppose $f_1, f_2 \in \mathbb{C}[x]$ satisfy $\deg f_1 > 1, \deg f_2 > 1$ and f_2 is indecomposable. Then f_1 and f_2 have a common composite if and only if there are linear polynomials $\ell_1, \ell_2, \ell_3 \in \mathbb{C}[x]$ such that one of the following holds:*

- *$f_1(x) = \ell_1(x) \circ x^r P(x^n) \circ \ell_3(x)$ and $f_2(x) = \ell_2(x) \circ x^n \circ \ell_3(x)$, where $r, n > 0$, $P \in \mathbb{C}[x]$, $\gcd(\deg f_1, \deg f_2) = 1$ and n is prime.*
- *$f_1(x) = \ell_1(x) \circ x^n \circ \ell_3(x)$ and $f_2(x) = \ell_2(x) \circ x^r P(x^n) \circ \ell_3(x)$, where $r, n > 0$, $P \in \mathbb{C}[x]$, $\gcd(\deg f_1, \deg f_2) = 1$ and $x^r P(x^n)$ is indecomposable, so in particular $\gcd(r, n) = 1$.*
- *$f_1(x) = \ell_1(x) \circ D_m(x, \alpha) \circ \ell_3(x)$, $f_2(x) = \ell_2(x) \circ D_n(x, \alpha) \circ \ell_3(x)$, where $m, n > 1$, $\alpha \in \mathbb{C}$, $\gcd(\deg f_1, \deg f_2) = 1$ and n is prime.*
- *$f_1(x) \in \mathbb{C}[f_2(x)]$.*

3. Preliminaries and auxiliary results

Our strategy involves the use of height functions in function fields. In what follows, let L be a finite extension of the rational function field $\mathbb{C}(x)$. For $a \in \mathbb{C}$ define the valuation v_a as follows. For $q(x) \in \mathbb{C}(x)$ let $q(x) = (x-a)^{v_a(q)} A(x)/B(x)$, where $A, B \in \mathbb{C}[x]$ and $A(a)B(a) \neq 0$. Furthermore, denote by v_∞ the (only) infinite valuation which is defined by $v_\infty(Q) := \deg B - \deg A$ for $Q(x) = A(x)/B(x)$, where $A, B \in \mathbb{C}[x]$. These are all (normalized) discrete valuations on $\mathbb{C}(x)$. All

of them can be extended in at most $[L : \mathbb{C}(x)]$ ways to a discrete valuation on L and again in this way one obtains all discrete valuations on L. Furthermore, for $f \in L^*$ the sum formula $\sum \nu(f) = 0$ holds, where the sum is taken over all discrete valuations on L. We just mention that there are different equivalent descriptions of the notion of discrete valuations as e.g. places or the rational points on a(ny) nonsingular complete curve over $\mathbb{C}$ with function field L.

Now, define the *projective height* $\mathcal{H}$ of $u_1, \ldots, u_n \in L/\mathbb{C}(x)$, where $n \geq 2$ and not all u_i zero, via

$$\mathcal{H}(u_1, \ldots, u_n) = -\sum_{\nu} \min(\nu(u_1), \ldots, \nu(u_n)). \tag{7}$$

Also, for a single element $f \in L^*$, we set

$$\mathcal{H}(f) = -\sum_{\nu} \min(0, \nu(f)). \tag{8}$$

In both cases the sum is taken over all discrete valuations ν on L. Note that $\nu(f) \neq 0$ only for a finite number of valuations ν and that $\mathcal{H}(f) = \sum_{\nu} \max(0, \nu(f))$ if $f \in L^*$, by the sum formula. For $f = 0$, we define $\mathcal{H}(f) = \infty$. We call a a *zero* of f if $\nu_a(f) > 0$ and a *pole* of f if $\nu_a(f) < 0$. We state some basic properties of the projective height.

Lemma 2. *Denote as above by $\mathcal{H}$ the projective height on $L/\mathbb{C}(x)$. Then for $f, g \in L^*$ the following properties hold:*

(1) $\mathcal{H}(f) \geq 0$ and $\mathcal{H}(f) = \mathcal{H}(1/f)$,
(2) $\mathcal{H}(f) - \mathcal{H}(g) \leq \mathcal{H}(f + g) \leq \mathcal{H}(f) + \mathcal{H}(g)$,
(3) $\mathcal{H}(f) - \mathcal{H}(g) \leq \mathcal{H}(fg) \leq \mathcal{H}(f) + \mathcal{H}(g)$,
(4) $\mathcal{H}(f^n) = |n| \cdot \mathcal{H}(f)$,
(5) $\mathcal{H}(f) = 0 \Leftrightarrow f \in \mathbb{C}^*$,
(6) $\mathcal{H}(A(f)) = \deg A \cdot \mathcal{H}(f)$ for any $A \in \mathbb{C}[T]\backslash\{0\}$.

Proof. $\mathcal{H}(f) \geq 0$ clearly holds by definition. To show that $\mathcal{H}(f + g) \leq \mathcal{H}(f) + \mathcal{H}(g)$, note that $\min(0, \nu(f + g)) \geq \min(0, \nu(f)) + \min(0, \nu(g))$. Namely, if $\min(0, \nu(f + g)) = 0$, this clearly holds. Otherwise, by the definition of discrete valuations we have $\nu(f + g) \geq \min(\nu(f), \nu(g))$ and it follows that $\min(0, \nu(f + g)) = \nu(f + g) \geq \min(0, \nu(f)) + \min(0, \nu(g))$. Hence, $\mathcal{H}(f+g) = -\sum_{\nu} \min(0, \nu(f+g)) \leq -\sum_{\nu} \min(0, \nu(f)) - \sum_{\nu} \min(0, \nu(g)) = \mathcal{H}(f) + \mathcal{H}(g)$. Similarly, $\mathcal{H}(fg) \leq \mathcal{H}(f) + \mathcal{H}(g)$ follows from $\nu(fg) = \nu(f) + \nu(g)$.

We now show that $\mathcal{H}(f) = \mathcal{H}(1/f)$. Since $f \neq 0$, clearly $\nu(f^{-1}) = -\nu(f)$ and therefore we have $\min(0, \nu(f)) = -\max(0, \nu(f^{-1}))$. By the sum formula it follows that $\mathcal{H}(f) = -\sum_{\nu} \min(0, \nu(f)) = \sum_{\nu} \max(0, \nu(f^{-1})) = -\sum_{\nu} \min(0, \nu(f^{-1})) = \mathcal{H}(f^{-1})$.

Next we show that $\mathcal{H}(f) - \mathcal{H}(g) \leq \mathcal{H}(fg)$. We have $\mathcal{H}(f) = \mathcal{H}(fgg^{-1}) \leq \mathcal{H}(fg) + \mathcal{H}(g^{-1}) = \mathcal{H}(fg) + \mathcal{H}(g)$, so $\mathcal{H}(fg) \geq \mathcal{H}(f) - \mathcal{H}(g)$. Analogously, one concludes $\mathcal{H}(f + g) \geq \mathcal{H}(f) - \mathcal{H}(g)$.

For $n \in \mathbb{N}_0$, the identity $\mathcal{H}(f^n) = |n| \cdot \mathcal{H}(f)$ follows immediately from the definition of discrete valuations. Since $\mathcal{H}(f^n) = \mathcal{H}(f^{-n})$, the statement also holds for negative integers n.

By [23, Cor. I.1.19, p. 8], any transcendental element $f \in L$ has at least one zero and one pole. So if f is transcendental, there is a valuation ν on L such that $\nu(f) < 0$ and consequently $\mathcal{H}(f) > 0$. On the other hand, $\mathcal{H}(f) = 0$ for any $f \in \mathbb{C}^*$.

To see that (6) holds, observe that by (2) and (3), it follows that if $a \in \mathbb{C}$, then $\mathcal{H}(af) = \mathcal{H}(f + a) = \mathcal{H}(f)$. We argue by induction on $n = \deg A$. The statement holds for $n = 0$ since in this case $\mathcal{H}(A(f)) = 0 = \deg A \cdot \mathcal{H}(f)$. Also, if $n = 1$, and say $A(T) = aT + b$ where $a, b \in \mathbb{C}$, then $\mathcal{H}(A(f)) = \mathcal{H}(af + b) = \mathcal{H}(f) = \deg A \cdot \mathcal{H}(f)$. Let us now assume that $\deg A = n + 1$ and that the statement is true for lower-degree polynomials. If $A(T) = aT^{n+1} + b$, with $a, b \in \mathbb{C}$, the claimed equality clearly holds. Otherwise, let $m > 0$ be the unique integer such that $A(T) - A(0) = T^m A_1(T)$ and $A_1(T) \in \mathbb{C}[T]$ is such that $A_1(0) \neq 0$. Note that $\deg A_1 = n + 1 - m$, so that we can apply the induction hypothesis to A_1. We claim that

$$\max(0, \nu(f^m) + \nu(A_1(f))) = \max(0, \nu(f^m)) + \max(0, \nu(A_1(f))).$$

Indeed, if $\nu(f^m) > 0$ then $\nu(f) > 0$, and by the strict triangle inequality for valuations it follows that $\nu(A_1(f)) = 0$ for $A_1(0) \neq 0$. On the other hand, if $\nu(f^m) < 0$, and consequently $\nu(f) < 0$, then (again by the strict triangle inequality) we have $\nu(A_1(f)) < 0$. So the claimed equality holds in any case. We conclude

$$\begin{aligned}
\mathcal{H}(A(f)) = \mathcal{H}(A(f) - A(0)) = \mathcal{H}(f^m A_1(f)) &= \sum_\nu \max(0, \nu(f^m A_1(f))) \\
&= \sum_\nu \max(0, \nu(f^m) + \nu(A_1(f))) \\
&= \sum_\nu \left[\max(0, \nu(f^m)) + \max(0, \nu(A_1(f)))\right] \\
&= \mathcal{H}(f^m) + \mathcal{H}(A_1(f)) = m \cdot \mathcal{H}(f) + (n + 1 - m) \cdot \mathcal{H}(f) \\
&= \deg A \cdot \mathcal{H}(f).
\end{aligned}$$

□

We use the following result due to Brownawell and Masser taken from [13] (more precisely, this is a direct consequence of [5, Thm. B and Cor. 1]), which gives an upper bound for the height of S-units, which arise as a solution of certain S-unit-equations. Recall that for a set S of discrete valuations, we call an element of L an *S-unit*, if it has poles and zeros only at places in S, or equivalently, the set of S-units in L is

$$\mathcal{O}_S^* = \{f \in L : \nu(f) = 0 \text{ for all } \nu \notin S\}.$$

Theorem 3. *(Brownawell-Masser) Let $F/\mathbb{C}$ be a function field of one variable of genus $\mathfrak{g}$. Moreover, let $u_1, \ldots, u_n$ be not all constant S-units for a finite set S of discrete valuations, and*

$$1 + u_1 + u_2 + \ldots + u_n = 0,$$

where no proper subsum of the left side vanishes. Then it holds

$$\max_{i=1,\ldots,n} \mathcal{H}(u_i) \leq \frac{1}{2}(n-1)(n-2)(|S| + 2\mathfrak{g} - 2). \tag{9}$$

Furthermore, we use the following classical estimates for the genus of a compositum of function fields, which are taken from [23, p. 130, p. 132].

Theorem 4. *(Castelnuovo's Inequality) Let $F/\mathbb{C}$ be a function field of one variable of genus $\mathfrak{g}$. Suppose there are given two subfields $F_1/\mathbb{C}$ and $F_2/\mathbb{C}$ of $F/\mathbb{C}$ satisfying*

(1) $F = F_1F_2$ is the compositum of F_1 and F_2.
(2) $[F : F_i] = n_i$, and $F_i/\mathbb{C}$ has genus $\mathfrak{g}_i$ $(i = 1, 2)$.

Then we have

$$\mathfrak{g} \leq n_1\mathfrak{g}_1 + n_2\mathfrak{g}_2 + (n_1 - 1)(n_2 - 1).$$

Theorem 5. *(Riemann's Inequality) Suppose that $F = \mathbb{C}(x, y)$. Then we have the following estimate for the genus $\mathfrak{g}$ of $F/\mathbb{C}$:*

$$\mathfrak{g} \leq ([F : \mathbb{C}(x)] - 1)([F : \mathbb{C}(y)] - 1).$$

We now prove three lemmas that we will need in the proofs of our main results.

Lemma 3. *Let $h \in \mathbb{C}[x]$ be indecomposable and let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$. If h is neither cyclic nor dihedral, then*

$$[\mathbb{C}(x, y) : \mathbb{C}(x)] \geq \frac{1}{2}\deg h.$$

Proof. We set $d = [\mathbb{C}(x, y) : \mathbb{C}(x)]$. Then d is the degree of a minimal polynomial $\tilde{H}(Y) \in \mathbb{C}(x)[Y]$ of y over $\mathbb{C}(x)$. Let $H(X, Y) = (h(X) - h(Y))/(X - Y) \in \mathbb{C}[X, Y]$. Then $H(x, Y) \in \mathbb{C}(x)[Y]$ is a polynomial in Y for which $H(x, y) = 0$ holds. It follows that $\tilde{H}(Y)$ divides $H(x, Y)$.

If $H_1(X, Y) \in \mathbb{C}[X, Y]$ is any irreducible polynomial such that $H_1(x, y) = 0$, then $H_1(X, Y)|H(X, Y)$. Then the highest homogeneous part of $H_1(X, Y)$ divides the highest homogeneous part of $H(X, Y)$, which is a constant multiple of

$$\frac{X^{\deg h} - Y^{\deg h}}{X - Y} = X^{\deg h - 1} + X^{\deg h - 2}Y + \cdots + XY^{\deg h - 2} + Y^{\deg h - 1}.$$

Therefore, it follows $\deg H_1 = \deg_X H_1 = \deg_Y H_1 = d$. This argument can be found in the proof of [26, Lemma 3].

Since h is neither cyclic nor dihedral, if $\deg h \geq 3$, according to Fried [7] it follows that $H(X, Y) = (h(X) - h(Y))/(X - Y) \in \mathbb{C}[X, Y]$ is irreducible. (See

also Turnwald's paper [24, Thm. 4.5] for a detailed exposition of Fried's proof.) Then H is a constant multiple of H_1 and we conclude

$$\deg h - 1 = \deg H = \deg H_1 = \deg_Y H_1 = d.$$

Thus, $[\mathbb{C}(x, y) : \mathbb{C}(x)] = \deg h - 1 \geq \deg h/2$. If $\deg h = 2$, we clearly have $[\mathbb{C}(x, y) : \mathbb{C}(x)] \geq 1 = \deg h/2$. □

Lemma 4. *Let $h \in \mathbb{C}[x]$ be indecomposable and let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$. Then either $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$ and h is cyclic or $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$.*

Proof. By assumption, $h(x) = h(y)$. Note that thus $\mathbb{C}(h(x)) \subseteq \mathbb{C}(x) \cap \mathbb{C}(y) \subseteq \mathbb{C}(x)$. By Lüroth's theorem (see [22, p. 13]) it follows that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(r(x))$ for some $r \in \mathbb{C}(x)$. Moreover, since h is a polynomial, r can be chosen to be a polynomial as well by [22, p. 16]. Assume henceforth $r \in \mathbb{C}[x]$. Then $h(x) \in \mathbb{C}[r(x)]$. Since h is indecomposable, it follows that either $\deg r = \deg h$ or $\deg r = 1$, i.e. that either $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$ or $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$. Note that if $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$, then $\nu(y) = x$ for some $\nu \in \mathbb{C}(x)$. Furthermore, clearly $h(\nu(y)) = h(x) = h(y)$. We deduce that $\nu \in \mathbb{C}[x]$.

Let $\mathrm{Aut}(h)$ denote the group of linear polynomials $\ell \in \mathbb{C}[x]$ such that $h \circ \ell = h$. It follows that $\nu \in \mathrm{Aut}(h)$ and since $\nu(y) = x \neq y$, it follows that $\mathrm{Aut}(h)$ is a non-trivial group. Recall that h is by assumption indecomposable. We now show that $\mathrm{Mon}(h)$ is cyclic, and hence that h is cyclic. This has been shown in Remark 2.14 in [20], as well as in Corollary 6.6 in [17]. For the sake of completeness we recall the proof.

First recall from Sect. 2 that if L is the splitting field of $h(X) - t$ over $\mathbb{C}(t)$ and x is such that $h(x) = t$, then $G := \mathrm{Mon}(h) = \mathrm{Gal}(L/\mathbb{C}(h(x)))$, and if we set $H = \mathrm{Gal}(L/\mathbb{C}(x))$, then $G = HI$ for some cyclic group I. Now note that $\mathrm{Aut}(h) \cong N_G(H)/H$. Since h is indecomposable, there are no intermediate fields between $\mathbb{C}(h(x))$ and $\mathbb{C}(x)$, and thus no proper subgroups between H and G, so either $N_G(H) = G$ or $N_G(H) = H$. In the latter case, $\mathrm{Aut}(h)$ is trivial, a contradiction. Thus $H \trianglelefteq G$. Since H contains no nontrivial normal subgroups of G (because L is the normal closure of $\mathbb{C}(x)/\mathbb{C}(h(x))$), we must have $H = 1$, and $G = HI = I$, so G is cyclic. By Proposition 2 it follows that h is cyclic. □

Lemma 5. *Let $h \in \mathbb{C}[x]$ be indecomposable and let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$. Then the following hold.*

(1) For $q \in \mathbb{C}[h(x)]$ we have $q(x) = q(y)$. Furthermore, if h is not cyclic and $q(x) = q(y)$ for some $q \in \mathbb{C}[x]$, then $q \in \mathbb{C}[h(x)]$.
(2) Let $d := [\mathbb{C}(x, y) : \mathbb{C}(x)]$. Then $d \leq \deg h - 1$.
(3) The genus of the function field $\mathbb{C}(x, y)$ (over $\mathbb{C}$) is not greater than $(d-1)(d-2)/2$.

Zannier [26, Lemma 3] showed that for an arbitrary $h \in \mathbb{C}[x]$ with $\deg h \geq 1$, there exists a conjugate y of x over $\mathbb{C}(h(x))$ with the above properties: (1) then states that for $q \in \mathbb{C}[x]$, we have $q(x) = q(y)$ if and only if $q \in \mathbb{C}[h(x)]$, while (2) and (3) are the same as above. Note that in Lemma 5, we put some conditions on h, but y is an arbitrary conjugate of x (such that $y \neq x$).

Proof of Lemma 5. The first statement follows from $h(x) = h(y)$. Assume now that h is not cyclic and that $q(x) = q(y)$ for some $q \in \mathbb{C}[x]$. By Lemma 4 it follows that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Since $q(x) = q(y)$, it follows that $q(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Furthermore, since $h, q \in \mathbb{C}[x]$, we have $q(x) \in \mathbb{C}[h(x)]$. This completes the proof of (1). We prove the other two statements completely analogously to the proof of Lemma 3 from [26]. By setting $H(X, Y) := (h(X) - h(Y)/(X - Y)$ we have $H(x, y) = 0$. Then (2) follows from $\deg_Y H \leq \deg H = \deg h - 1$. If $H_1(X, Y) \in \mathbb{C}[X, Y]$ is any irreducible polynomial such that $H_1(x, y) = 0$, then one shows by the same argument as in the proof of Lemma 3 that $\deg H_1 = \deg_X H_1 = \deg_Y H_1 = d$. Then (3) is a consequence of the fact that the genus of a plane curve of degree $\leq d$ is bounded by $(d - 1)(d - 2)/2$. □

4. Proof of Theorem 2

In this section we prove Theorem 2 using results from the previous two sections. Recall that $A_0, A_1, G_0, G_1 \in \mathbb{C}[x]$ and $(G_n)_{n=0}^{\infty}$ is a sequence of polynomials defined by the minimal non-degenerate simple linear recurrence

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x), \quad n \in \mathbb{N}.$$

We are assuming that for some n we have $G_n = g \circ h$, where h is indecomposable, and that x and y, which define equation 4, are such that $h(x) = h(y)$ and $x \neq y$. We will use this notation throughout this section. In this notation, we have the following characterization of the existence of a proper vanishing subsum of (4) in the case when $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Note that by Lemma 4, either this holds or h is cyclic.

Lemma 6. *If $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, then there exists a proper vanishing subsum of (4) if and only if $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(h(x))$.*

Note that we have $\alpha_1 + \alpha_2 = A_1(x)$ and $\alpha_1\alpha_2 = -A_0(x)$ by Vieta's formulae. Clearly, $G_0(x) = \pi_1 + \pi_2$ and $G_1(x) = \pi_1\alpha_1 + \pi_2\alpha_2$. Then

$$\pi_1 = \frac{G_1(x) - \alpha_2 G_0(x)}{\alpha_1 - \alpha_2}, \quad \pi_2 = -\frac{G_1(x) - \alpha_1 G_0(x)}{\alpha_1 - \alpha_2}, \tag{10}$$

and hence

$$\pi_1\pi_2 = -\frac{G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2}{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}(x). \tag{11}$$

Analogously,

$$\rho_1\rho_2 = -\frac{G_1(y)^2 - G_0(y)G_1(y)A_1(y) - A_0(y)G_0(y)^2}{A_1(y)^2 + 4A_0(y)} \in \mathbb{C}(y). \tag{12}$$

Proof of Lemma 6. There exists a proper vanishing subsum of (4) if and only if there exists a permutation σ of the set $\{1, 2\}$ such that

$$\pi_i \alpha_i^n = \rho_{\sigma(i)} \beta_{\sigma(i)}^n \tag{13}$$

for $i = 1, 2$. If there exists such a permutation, then in particular we have $\pi_1\pi_2 A_0(x)^n = \rho_1\rho_2 A_0(y)^n$, by Vieta's formulae. Since $\pi_1\pi_2 \in \mathbb{C}(x)$ and $A_0(x) \in \mathbb{C}(x)$ we have that $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(x)$. Analogously $\rho_1\rho_2 A_0(y)^n \in \mathbb{C}(y)$, so $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$.

Assume now that $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(h(x))$, so that $\pi_1\pi_2 A_0(x)^n = p(h(x))$ for some $p \in \mathbb{C}(x)$. Then analogously $\rho_1\rho_2 A_0(y)^n = p(h(y))$ and since $h(x) = h(y)$ we get $\pi_1\pi_2 A_0(x)^n = \rho_1\rho_2 A_0(y)^n$. Since $G_n(x) = G_n(y)$ it follows that

$$G_n(x)^2 - 4\pi_1\pi_2(-A_0(x))^n = G_n(y)^2 - 4\rho_1\rho_2(-A_0(y))^n,$$

and hence

$$\pi_1\alpha_1^n - \pi_2\alpha_2^n = \pm(\rho_1\beta_1^n - \rho_2\beta_2^n).$$

Thus, there exists a proper vanishing subsum of (4). □

Note that by Lemma 4 and Lemma 6 it follows that if $A_0(x) = a_0 \in \mathbb{C}$ and

$$\pi_1\pi_2 = -\frac{G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2}{A_1(x)^2 + 4A_0(x)} = \pi \in \mathbb{C},$$

then either h is cyclic or there exists a proper vanishing subsum of (4). On the other hand, we have the following.

Lemma 7. *If $\pi_1\pi_2 = \pi A_0(x)^m$ for some $m \geq 0$, $\pi \in \mathbb{C}$ and $\deg A_0 = 1$, then either h is cyclic or there does not exist a proper vanishing subsum of (4).*

Proof. By $\pi_1\pi_2 = \pi A_0(x)^m$ and by Lemma 4 and Lemma 6, it follows that if there exists a proper vanishing subsum of (4), then either h is cyclic or $A_0(x)^{m+n} \in \mathbb{C}[h(x)]$. Assuming the latter, by Lemma 5 we have $A_0(x) = \zeta A_0(y)$ for some $(m+n)$-th root of unity ζ. Then $A_0(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Since $\deg A_0 = 1$ and $\deg h \geq 2$, we have a contradiction. □

In Theorem 2 we are assuming that we do not have $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$. We have the following characterization of this situation.

Lemma 8. *We have that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$ if and only if $G_0, G_1, A_0, A_1 \in \mathbb{C}[h(x)]$.*

Proof. Note that if $G_0, G_1, A_0, A_1 \in \mathbb{C}[h(x)]$ for some polynomial $h \in \mathbb{C}[x]$, then by the recurrence relation it follows that $G_m(x) \in \mathbb{C}[h(x)]$ for every $m \in \mathbb{N}$.

Conversely, assume that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$. If G_0, G_1, G_2, G_3 (or any four consecutive elements of the sequence) satisfy $G_1^2 - G_0G_2 \neq 0$, then the linear system $G_2 = A_1G_1 + A_0G_0$, $G_3 = A_1G_2 + A_0G_1$ shows that

$$A_0 = \frac{G_1G_3 - G_2^2}{G_1^2 - G_0G_2}, \quad A_1 = \frac{G_1G_2 - G_0G_3}{G_1^2 - G_0G_2}$$

and hence $A_0(x)$, $A_1(x)$ are in $\mathbb{C}(h(x)) \cap \mathbb{C}[x] = \mathbb{C}[h(x)]$ (the last equality follows immediately by integrality). Since $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$ it cannot always hold that $G_{m+1}^2 = G_m G_{m+2}$ because in this case a short calculation shows that

$$G_{m+1} = \left(A_1 \pm \sqrt{A_1^2 + 4A_0}\right) G_m/2,$$

contradicting the assumption that $(G_n)_{n=0}^{\infty}$ is a second order linear recurrence (observe that in this case necessarily $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$). □

Lemma 9. *If h is not cyclic and if $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$, then (4) has a proper vanishing subsum.*

Proof. Since h is not cyclic, by Lemma 4 it follows that $C(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Assume that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \in \mathbb{N}$. Then by Lemma 8 it follows that $G_0(x)$, $G_1(x)$, $A_0(x)$, $A_1(x) \in \mathbb{C}[h(x)]$. From (11) we conclude that $\pi_1\pi_2 \in \mathbb{C}(h(x))$ and hence $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(h(x))$. By Lemma 6 it follows that (4) has a proper vanishing subsum. □

We complete a proof of Theorem 2 with the help of two lemmas. First note that by (10) it follows that $\pi_1 = \pi_2$ if and only if $2G_1(x) = G_0(x)A_1(x)$.

Lemma 10. *If h is neither dihedral nor cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, then (4) has no proper vanishing subsum if $A_0(x)$ is constant and $2G_1(x) = G_0(x)A_1(x)$, i.e. $\pi_1 = \pi_2$.*

Furthermore, if h is not cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, then (4) has no proper vanishing subsum if $\pi_1 = \pi_2 = \pi \in \mathbb{C}$ and either $\deg A_0 = 1$ *or* $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$.

Proof. Assume that h is not cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, and that there exists a proper vanishing subsum of (4). Recall that by Lemma 4 and Lemma 6 it follows that $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(h(x))$.

Assume first that $A_0(x) = a_0 \in \mathbb{C}$ and $\pi_1 = \pi_2 =: \pi$. Then $G_0(x) = 2\pi$ and since $A_0(x) = a_0 \in \mathbb{C}$, it follows that

$$\pi_1\pi_2 A_0(x)^n = \frac{a_0^n G_0(x)^2}{4} \in \mathbb{C}(h(x)),$$

and hence $G_0(x)^2 \in \mathbb{C}(h(x))$. Then $G_0(x)^2 = G_0(y)^2$ by Lemma 5, so $G_0(x) = \pm G_0(y)$. Thus, $G_0(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Moreover, $G_0(x) \in \mathbb{C}(h(x)) \cap \mathbb{C}[x] = \mathbb{C}[h(x)]$.

Furthermore, by Proposition 3 we have

$$G_n(x) = \pi(\alpha_1^n + \alpha_2^n) = \frac{1}{2} G_0(x) D_n(A_1(x), -a_0) \in \mathbb{C}[h(x)].$$

Since $G_0(x) \in \mathbb{C}[h(x)]$, it follows that $D_n(A_1(x), -a_0) \in \mathbb{C}[h(x)]$. Observe that $\deg A_1 > 1$. Namely, if $A_1(x) = a_1 \in \mathbb{C}$, since $G_0(x) \in \mathbb{C}[h(x)]$ it follows that for any $m \in \mathbb{N}$ we have that

$$G_m(x) = \frac{1}{2} G_0(x) D_m(a_1, -a_0) \in \mathbb{C}[h(x)],$$

a contradiction with the assumption. If $\deg A_1 = 1$, we have

$$G_n(x) = \frac{1}{2} G_0(x) D_n(A_1(x), -a_0).$$

Since $G_n(x),\ G_0(x) \in \mathbb{C}[h(x)]$, it follows that

$$D_n(A_1(x), -a_0) \in \mathbb{C}(h(x)) \cap \mathbb{C}[x] = \mathbb{C}[h(x)].$$

Obviously, $D_n(A_1(x), -a_0)$ is equivalent to $D_n(x, -a_0)$, which is either cyclic or dihedral. By Lemma 1, Proposition 1 and Proposition 2 it follows that h is either cyclic or dihedral, a contradiction with the assumption. We conclude that $\deg A_1, \deg h > 1$ and A_1 and h have a common composite. We now use Proposition 4. If $A_1(x) \in \mathbb{C}[h(x)]$, since $G_0(x) \in \mathbb{C}[h(x)]$ it follows that for any $m \in \mathbb{N}$ we have

$$G_m(x) = \frac{1}{2} G_0(x) D_m(A_1(x), -a_0) \in \mathbb{C}[h(x)],$$

a contradiction with the assumption. Assume thus that $A_1(x) \notin \mathbb{C}[h(x)]$. By Proposition 4, since h is neither cyclic nor dihedral it follows that

$$h(x) = \ell_2(x) \circ x^r P(x^s) \circ \ell_3(x), \quad A_1(x) = \ell_1(x) \circ x^s \circ \ell_3(x)$$

for some linear polynomials $\ell_1, \ell_2, \ell_3 \in \mathbb{C}[x]$ and $s, r \in \mathbb{N}, s \geq 2$. In particular, A_1 is cyclic. By Proposition 1 and Lemma 1 it follows that the collection of monodromy groups in any complete decomposition of $D_n(A_1(x), -a_0)$ consists only of cyclic or dihedral groups. Since $D_n(A_1(x), -a_0) \in \mathbb{C}[h(x)]$, by Proposition 2 it follows that h is either cyclic or dihedral, a contradiction.

We now prove the second statement. Assume that $\pi_1 = \pi_2 = \pi \in \mathbb{C}$ and either $\deg A_0 = 1$ or $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$. Then

$$G_0(x) = 2\pi, \quad G_m(x) = \pi D_m(A_1(x), -A_0(x)) \quad \text{for } m \in \mathbb{N}.$$

Recall that by Lemma 4 and Lemma 6 it again follows that

$$\pi_1 \pi_2 A_0(x)^n = \pi^2 A_0(x)^n \in \mathbb{C}(h(x)) \cap \mathbb{C}[x] = \mathbb{C}[h(x)].$$

It follows that $A_0(x)^n \in \mathbb{C}[h(x)]$ and thus $A_0(x)^n = A_0(y)^n$ by Lemma 5. Then $A_0(x) = \zeta A_0(y)$ for some n-th root of unity ζ, so $A_0(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and moreover $A_0(x) \in \mathbb{C}[h(x)]$. In particular, $A_0(x) = A_0(y)$. If $\deg A_0 = 1$ we have a contradiction since $\deg h \geq 2$.

Thus $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$. Since

$$D_n(A_1(x), -A_0(x)) = \frac{1}{\pi} G_n(x) \in \mathbb{C}[h(x)],$$

by Lemma 5 we have

$$D_n(A_1(x), -A_0(x)) = D_n(A_1(y), -A_0(y)).$$

Since $A_0(x) = A_0(y)$ we further get

$$D_n(A_1(x), -A_0(x)) = D_n(A_1(y), -A_0(x)).$$

Using Proposition 3 we get that either $A_1(x) = \pm A_1(y)$ or

$$A_1(x)^2 - \gamma_k A_1(x)A_1(y) + A_1(y)^2 - \delta_k^2 A_0(x) = 0, \tag{14}$$

for $\gamma_k, \delta_k \in \mathbb{C}$ given in the proposition. If $A_1(x) = \pm A_1(y)$, then we have $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Then clearly $A_1(x) \in \mathbb{C}[(h(x)]$. Since also $A_0(x) \in \mathbb{C}[h(x)]$ we have that for any m

$$G_m(x) = \pi D_m(A_1(x), -A_0(x)) \in \mathbb{C}[h(x)],$$

a contradiction with the assumption. Thus we get that (14) holds. A short calculation shows that

$$A_1(x) = \frac{\gamma_k A_1(y) \pm \delta_k \sqrt{A_1(y)^2 + 4A_0(y)}}{2}.$$

Since $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$, we have that $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Moreover, $A_1(x) \in \mathbb{C}[h(x)]$. Then $A_1(x) = A_1(y)$, a contradiction with the assumption. □

Lemma 11. *If h is neither dihedral nor cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, then (4) has no proper vanishing subsum if $A_0(x)$ is constant, $G_0(x) = A_1(x)$, and either $G_1(x) = 2A_0(x) + G_0(x)^2$ or $G_1(x) = -2A_0(x)$.*

Furthermore, if h is not cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, then (4) has no proper vanishing subsum if $G_0(x) = A_1(x)$ and any of the following holds:

i) $G_1(x) = 2A_0(x) + G_0(x)^2$, *and*
either $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ *or* $\deg A_0 = 1$,
ii) $G_1(x) = -2A_0(x)$, *and*
either $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$ *or* $\deg A_0 = 1$.

Proof. Assume that h is not cyclic, and it does not hold that $G_m(x) \in \mathbb{C}[h(x)]$ for all m, and that there exists a proper vanishing subsum of (4). Recall that by Lemma 4 and Lemma 6 it follows that $\pi_1\pi_2 A_0(x)^n \in \mathbb{C}(h(x))$.

Assume further that $G_0(x) = A_1(x)$, and either $G_1(x) = 2A_0(x) + G_0(x)^2$ or $G_1(x) = -2A_0(x)$. Then

$$\pi_1 + \pi_2 = G_0(x) = A_1(x) = \alpha_1 + \alpha_2$$
$$\pi_1\pi_2 = -\frac{G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2}{A_1(x)^2 + 4A_0(x)} = -A_0(x) = \alpha_1\alpha_2.$$

Thus, either $\pi_1 = \alpha_1$ and $\pi_2 = \alpha_2$, or $\pi_1 = \alpha_2$ and $\pi_2 = \alpha_1$. In both cases,

$$\pi_1\pi_2 A_0(x)^n = -A_0(x)^{n+1} \in \mathbb{C}(h(x)).$$

Then $A_0(x)^{n+1} \in \mathbb{C}(h(x)) \cap \mathbb{C}[x] = \mathbb{C}[h(x)]$. By Lemma 5 it follows that $A_0(x)^{n+1} = A_0(y)^{n+1}$. Then $A_0(x) = \zeta A_0(y)$ for some $(n+1)$-st root of unity ζ, so $A_0(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and moreover $A_0(x) \in \mathbb{C}[h(x)]$. In particular, $A_0(x) = A_0(y)$.

Since either $\pi_1 = \alpha_1$ and $\pi_2 = \alpha_2$, or $\pi_1 = \alpha_2$ and $\pi_2 = \alpha_1$, by Proposition 3 we have

$$G_m(x) = \begin{cases} D_{m+1}(A_1(x), -A_0(x)), & \text{if } \pi_1 = \alpha_1,\ \pi_2 = \alpha_2 \\ -A_0(x) D_{m-1}(A_1(x), -A_0(x)), & \text{if } \pi_1 = \alpha_2,\ \pi_2 = \alpha_1. \end{cases} \tag{15}$$

for any m. Since $A_0(x) \in \mathbb{C}[h(x)]$ and $G_n(x) \in \mathbb{C}[h(x)]$ it follows that for some $i \in \{n-1, n+1\}$ we have

$$D_i(A_1(x), -A_0(x)) \in \mathbb{C}[h(x)], \tag{16}$$

and consequently by Lemma 5 that

$$D_i(A_1(x), -A_0(x)) = D_i(A_1(y), -A_0(x)).$$

Then either $A_1(x) = \pm A_1(y)$ or

$$A_1(x)^2 - \gamma_k A_1(x) A_1(y) + A_1(y)^2 - \delta_k^2 A_0(x) = 0,$$

for some of γ_k, δ_k given in Proposition 3. If $A_1(x) = \pm A_1(y)$, then $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Then clearly $A_1(x) \in \mathbb{C}[(h(x)]$. Since also $A_0(x) \in \mathbb{C}[h(x)]$, by (15) we have that $G_m(x) \in \mathbb{C}[h(x)]$ for any m, a contradiction with the assumption. Thus we get that (14) holds. A short calculation shows that

$$A_1(x) = \frac{\gamma_k A_1(y) \pm \delta_k \sqrt{A_1(y)^2 + 4A_0(y)}}{2}.$$

If $\sqrt{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}[x]$, we have that $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Moreover, $A_1(x) \in \mathbb{C}[h(x)]$. Then $A_1(x) = A_1(y)$, a contradiction with the assumption. If $\deg A_0 = 1$ we have a contradiction with $A_0(x) \in \mathbb{C}[h(x)]$ since $\deg h \geq 2$.

It remains to examine the case when in addition to the assumptions stated at the beginning of the proof we have $A_0(x) = a_0 \in \mathbb{C}$ and h is not dihedral.

By (16) we have $D_i(A_1(x), -a_0) \in \mathbb{C}[h(x)]$. If $A_1(x) \in \mathbb{C}[h(x)]$, by (15) it follows that $G_m(x) \in \mathbb{C}[h(x)]$ for any $m \in \mathbb{N}$, a contradiction with the assumption. Assume thus that $A_1(x) \notin \mathbb{C}[h(x)]$. As in the proof of Lemma 10, we conclude $\deg A_1 > 1$. By Proposition 4, since h is neither cyclic nor dihedral it follows that

$$h(x) = \ell_2(x) \circ x^r P(x^s) \circ \ell_3(x), \quad A_1(x) = \ell_1(x) \circ x^s \circ \ell_3(x)$$

for some linear polynomials $\ell_1, \ell_2, \ell_3 \in \mathbb{C}[x]$ and $s, r \in \mathbb{N}, s \geq 2$. In particular, A_1 is cyclic. By Proposition 1 and Lemma 1 it follows that the collection of monodromy groups in any complete decomposition of $D_i(A_1(x), -a_0)$ consists only of cyclic or dihedral groups. Since $D_i(A_1(x), -a_0) \in \mathbb{C}[h(x)]$, by Proposition 2 it follows that h is either cyclic or dihedral, a contradiction. □

Proof of Theorem 2. By Lemma 7, Lemma 10 and Lemma 11 we conclude the proof of Theorem 2. □

5. Proof of Theorem 1

Proof of Theorem 1. Assume that $G_n(x) = g(h(x))$, where h is indecomposable and neither cyclic nor dihedral. Recall that x and y, which define (4), are such that $h(x) = h(y)$ and $x \neq y$. From Lemma 4 it follows that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Assume further that there is no proper vanishing subsum of (4) and write it as

$$1 - \frac{\pi_1 \alpha_1^n}{\rho_2 \beta_2^n} + \frac{\rho_1 \beta_1^n}{\rho_2 \beta_2^n} - \frac{\pi_2 \alpha_2^n}{\rho_2 \beta_2^n} = 0. \tag{17}$$

Define

$$u_1 = -\frac{\pi_1 \alpha_1^n}{\rho_2 \beta_2^n}, \quad u_2 = \frac{\rho_1 \beta_1^n}{\rho_2 \beta_2^n}, \quad u_3 = -\frac{\pi_2 \alpha_2^n}{\rho_2 \beta_2^n},$$

and also

$$v_1 = \frac{\alpha_1}{\beta_2}, \quad v_2 = \frac{\beta_1}{\beta_2}, \quad v_3 = \frac{\alpha_2}{\beta_2},$$
$$w_1 = \frac{\pi_1}{\rho_2}, \quad w_2 = \frac{\rho_1}{\rho_2}, \quad w_3 = \frac{\pi_2}{\rho_2}.$$

Let $F = \mathbb{C}(x, y, \alpha_1, \alpha_2, \beta_1, \beta_2)$ and let $\mathcal{H}$ be the projective height on $F/\mathbb{C}(x)$, defined as in Sect. 3. By Lemma 2, we find the estimate

$$\mathcal{H}\left(\frac{\pi_i \alpha_i^n}{\rho_2 \beta_2^n}\right) \geq n \cdot \mathcal{H}\left(\frac{\alpha_i}{\beta_2}\right) - \mathcal{H}\left(\frac{\pi_i}{\rho_2}\right), \quad i = 1, 2,$$

and similarly we argue for u_2. So, for $i = 1, 2, 3$, we have

$$\mathcal{H}(u_i) \geq n\mathcal{H}(v_i) - \mathcal{H}(w_i).$$

Note that if for some i we have $\mathcal{H}(v_i) \neq 0$, then

$$n \leq (\mathcal{H}(u_i) + \mathcal{H}(w_i)) \cdot \mathcal{H}(v_i)^{-1}.$$

Since $(G_n(x))_{n=0}^{\infty}$ is non-degenerate, the same holds for the sequence $(G_n(y))_{n=0}^{\infty}$, i.e. $\beta_1/\beta_2 \notin \mathbb{C}$. It follows that $\mathcal{H}(v_2) = \mathcal{H}(\beta_1/\beta_2) \neq 0$ and thus

$$n \leq (\mathcal{H}(u_2) + \mathcal{H}(w_2)) \cdot \mathcal{H}(v_2)^{-1}. \tag{18}$$

On the other hand, we find the following upper bound for the height of $G_n(x)$:

$$\begin{aligned} \mathcal{H}(G_n(x)) &= \mathcal{H}(\pi_1 \alpha_1^n + \pi_2 \alpha_2^n) \\ &\leq \mathcal{H}(\pi_1) + n\mathcal{H}(\alpha_1) + \mathcal{H}(\pi_2) + n\mathcal{H}(\alpha_2) \\ &\leq n(\mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2) + \mathcal{H}(\pi_1) + \mathcal{H}(\pi_2)). \end{aligned}$$

Using (18), we conclude that

$$\mathcal{H}(G_n(x)) \leq (\mathcal{H}(u_2) + \mathcal{H}(w_2))\, \mathcal{H}(v_2)^{-1} (\mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2) + \mathcal{H}(\pi_1) + \mathcal{H}(\pi_2)). \tag{19}$$

Now consider equation (17), which by assumption has no proper vanishing subsum. Let $A = \{\alpha_i, \pi_i, \beta_i, \rho_i, i = 1, 2\}$ and put

$$S := \{\nu \in S_0 : \ \nu(f) \neq 0 \text{ for some } f \in A\} \cup S_\infty,$$

where S_0 denotes the set of finite valuations and S_∞ denotes the set of infinite valuations on F. Then by Theorem 3 it follows that

$$\mathcal{H}(u_2) \leq |S| + 2\mathfrak{g} - 2, \tag{20}$$

where $\mathfrak{g}$ is the genus of $F/\mathbb{C}$. We now estimate the genus and $|S|$ in terms of $\deg h$. We start with the genus. In order to use Castelnuovo's inequality (Theorem 4), we define

$$F_1 = \mathbb{C}(x, \alpha_1, \alpha_2), \quad F_2 = \mathbb{C}(y, \beta_1, \beta_2).$$

Note that $\mathbb{C}$ is the field of constants of F_1, F_2 and that $F = F_1F_2$. Let $n_i := [F : F_i]$, $i = 1, 2$. Recall that the α_i's and β_i's are roots of a monic quadratic polynomial and that $[\mathbb{C}(x, y) : \mathbb{C}(x)] < \deg h$ by Lemma 5. Thus $n_i < 2 \deg h$. For $i = 1, 2$ let $\mathfrak{g}_i$ be the genus of $F_i/\mathbb{C}$. Note that since

$$\alpha_1 = \frac{A_1(x) - \sqrt{A_1(x)^2 + 4A_0(x)}}{2}, \quad \alpha_2 = \frac{A_1(x) + \sqrt{A_1(x)^2 + 4A_0(x)}}{2}, \tag{21}$$

we have that $\mathbb{C}(x, \alpha_1, \alpha_2) = \mathbb{C}(x, \sqrt{\Delta(x)})$, where $\Delta(x) = A_1(x)^2 + 4A_0(x)$. Now Riemann's inequality (Theorem 5) yields

$$\mathfrak{g}_1 \leq ([F_1 : \mathbb{C}(x)] - 1)([F_1 : \mathbb{C}(\sqrt{\Delta(x)})] - 1).$$

Since $\sqrt{\Delta(x)}$ is a root of $T^2 - \Delta(x) \in \mathbb{C}(x)[T]$ and x is a root of $\Delta(T) - \sqrt{\Delta(x)}^2 \in \mathbb{C}(\sqrt{\Delta(x)})[T]$, we conclude that

$$\mathfrak{g}_1 \leq (2 - 1) \cdot (\deg \Delta - 1) = \deg \Delta - 1 \leq C_1 - 1,$$

where $C_1 := \max\{\deg A_0, 2 \deg A_1\}$ (it will be shown later that indeed $C_1 \geq 1$, by the non-degeneracy of the sequence).

Since F_1 and F_2 are isomorphic function fields, they have the same genus and hence the same bound holds for $\mathfrak{g}_2$. Therefore we find that $\mathfrak{g}_i \leq C_1 - 1$, $i = 1, 2$. By Castelnuovo's inequality (Theorem 4) we get

$$\begin{aligned} \mathfrak{g} &\leq n_1\mathfrak{g}_1 + n_2\mathfrak{g}_2 + (n_1 - 1)(n_2 - 1) \\ &< 4 \deg h(C_1 - 1) + (2 \deg h - 1)^2 < 4C_1 \deg h^2. \end{aligned}$$

To estimate $|S|$, let

$$\begin{aligned} S_1 &= \{\nu \in S_0 : \ \nu(\alpha_1) \neq 0 \text{ or } \nu(\alpha_2) \neq 0\}, \\ S_2 &= \{\nu \in S_0 : \ \nu(\pi_1) \neq 0 \text{ or } \nu(\pi_2) \neq 0\}, \\ S_3 &= \{\nu \in S_0 : \ \nu(\beta_1) \neq 0 \text{ or } \nu(\beta_2) \neq 0\}, \\ S_4 &= \{\nu \in S_0 : \ \nu(\rho_1) \neq 0 \text{ or } \nu(\rho_2) \neq 0\}. \end{aligned}$$

Clearly, $|S| \le |S_1| + |S_2| + |S_3| + |S_4| + |S_\infty|$. Since $[F : \mathbb{C}(x)] < 4 \deg h$ we have $|S_\infty| < 4 \deg h$. For the other sets, we argue as follows.

Note that the α_i's are integral over $\mathbb{C}(x)$ (they are the roots of $\mathcal{G}(T)$) and therefore $\nu(\alpha_i) \ge 0$ for every finite valuation ν. Note that thus $\nu(\alpha_1\alpha_2) > 0$ if and only if either $\nu(\alpha_1) > 0$ or $\nu(\alpha_2) > 0$. Also, by Vieta's formulae we have $\alpha_1\alpha_2 = -A_0(x)$. Further recall that by Lemma 2 we have $\mathcal{H}(A_0(x)) = \deg A_0 \cdot \mathcal{H}(x)$ and that $\sum_\nu \max(0, \nu(A_0(x))) = \mathcal{H}(A_0(x))$ by the sum formula. Thus,

$$\begin{aligned}
|S_1| &= |\{\nu \in S_0 :\ \nu(\alpha_1) > 0 \text{ or } \nu(\alpha_2) > 0\}| \\
&= |\{\nu \in S_0 :\ \nu(\alpha_1\alpha_2) > 0\}| = |\{\nu \in S_0 :\ \nu(A_0(x)) > 0\}| \\
&\le \sum\nolimits' 1 \le \sum_\nu \max(0, \nu(A_0(x))) = \mathcal{H}(A_0(x)) \\
&= \deg A_0 \cdot \mathcal{H}(x) = \deg A_0 \cdot [F : \mathbb{C}(x)] < \deg A_0 \cdot 4 \deg h,
\end{aligned}$$

where the sum $\sum'$ runs over all valuations ν for which $\nu(A_0(x)) > 0$ holds.

In order to bound $|S_3|$ we argue similarly. We have that β_1, β_2 are the roots of the characteristic polynomial of $(G_n(y))_{n=0}^\infty$, and are hence integral over $\mathbb{C}(y)$. Since y is integral over $\mathbb{C}(x)$, we have that β_1, β_2 are integral over $\mathbb{C}(x)$. Therefore, as in the the case of S_1 we conclude that $\nu(\beta_i) \ge 0$ for every finite valuation ν. By Vieta's formulae we have $\beta_1\beta_2 = -A_0(y)$. Furthermore, since $h(x) = h(y)$ we have

$$\deg h \cdot \mathcal{H}(y) = \mathcal{H}(h(y)) = \mathcal{H}(h(x)) = \deg h \cdot \mathcal{H}(x),$$

and thus

$$\mathcal{H}(y) = \mathcal{H}(x) = [F : \mathbb{C}(x)].$$

Therefore,

$$\begin{aligned}
|S_3| &= |\{\nu \in S_0 :\ \nu(\beta_1) > 0 \text{ or } \nu(\beta_2) > 0\}| \\
&= |\{\nu \in S_0 :\ \nu(\beta_1\beta_2) > 0\}| = |\{\nu \in S_0 :\ \nu(A_0(y)) > 0\}| \\
&\le \deg A_0 \cdot \mathcal{H}(y) = \deg A_0 \cdot \mathcal{H}(x) < \deg A_0 \cdot 4 \deg h.
\end{aligned}$$

For $|S_2|$, note that

$$\begin{aligned}
|S_2| \le\ & |\{\nu \in S_0 :\ \nu(\pi_1) > 0 \text{ or } \nu(\pi_2) > 0\}| \\
& + |\{\nu \in S_0 :\ \nu(\pi_1) < 0 \text{ or } \nu(\pi_2) < 0\}|.
\end{aligned}$$

Recall that $G_0(x), G_1(x), \alpha_1, \alpha_2$ are integral over $\mathbb{C}(x)$, and thus also $G_1(x) - \alpha_2 G_0(x)$, $G_1(x) - \alpha_1 G_0(x)$ and $\alpha_1 - \alpha_2$. Therefore, for any $\nu \in S_0$ we have $\nu(G_1(x) - \alpha_2 G_0(x)) \ge 0$, $\nu(G_1(x) - \alpha_1 G_0(x)) \ge 0$ and $\nu(\alpha_1 - \alpha_2) \ge 0$. Thus

$$\begin{aligned}
\nu(\pi_1) &= \nu\left(\frac{G_1(x) - \alpha_2 G_0(x)}{\alpha_1 - \alpha_2}\right) \\
&= \nu(G_1(x) - \alpha_2 G_0(x)) + \nu\left(\frac{1}{\alpha_1 - \alpha_2}\right) \\
&= \underbrace{\nu(G_1(x) - \alpha_2 G_0(x))}_{\ge 0} - \underbrace{\nu(\alpha_1 - \alpha_2)}_{\ge 0}.
\end{aligned}$$

Hence for $\nu \in S_0$ it follows that

$$\nu(\pi_1) > 0 \text{ implies } \nu(G_1(x) - \alpha_2 G_0(x)) > 0,$$
$$\nu(\pi_1) < 0 \text{ implies } \nu(\alpha_1 - \alpha_2) > 0.$$

In the same manner we see that

$$\nu(\pi_2) > 0 \text{ implies } \nu(G_1(x) - \alpha_1 G_0(x)) > 0,$$
$$\nu(\pi_2) < 0 \text{ implies } \nu(\alpha_1 - \alpha_2) > 0.$$

Further note that since $\nu(G_1(x)-\alpha_2 G_0(x)) \geq 0$ and $\nu(G_1(x)-\alpha_1 G_0(x)) \geq 0$ for any $\nu \in S_0$ we have that either $\nu(G_1(x) - \alpha_2 G_0(x)) > 0$ or $\nu(G_1(x) - \alpha_1 G_0(x)) > 0$ if and only if

$$\nu((G_1(x) - \alpha_2 G_0(x))(G_1(x) - \alpha_1 G_0(x))) > 0,$$

that is

$$\nu(G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2) > 0.$$

In a similar manner we conclude that $\nu(\alpha_1-\alpha_2) > 0$ if and only if $\nu((\alpha_1-\alpha_2)^2) > 0$, that is

$$\nu(A_1(x)^2 + 4A_0(x)) > 0.$$

Therefore,

$$\begin{aligned}
|S_2| &\leq |\{\nu \in S_0 : \ \nu(\pi_1) > 0 \text{ or } \nu(\pi_2) > 0\}| \\
&\quad + |\{\nu \in S_0 : \ \nu(\pi_1) < 0 \text{ or } \nu(\pi_2) < 0\}| \\
&\leq |\{\nu \in S_0 : \ \nu(G_1(x) - \alpha_2 G_0(x)) > 0 \text{ or } \nu(G_1(x) - \alpha_1 G_0(x)) > 0\}| \\
&\quad + |\{\nu \in S_0 : \ \nu(\alpha_1 - \alpha_2) > 0\}| \\
&= |\{\nu \in S_0 : \nu(G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2) > 0\}| \\
&\quad + |\{\nu \in S_0 : \nu(A_1(x)^2 + 4A_0(x)) > 0\}|,
\end{aligned}$$

and then arguing similarly as for S_1 we get

$$\begin{aligned}
|S_2| &\leq \mathcal{H}((G_1^2 - G_0G_1A_1 - G_0^2A_0)(x)) + \mathcal{H}((A_1^2 + 4A_0)(x)) \\
&\leq (C_2 + C_1)\mathcal{H}(x) < (C_1 + C_2)4 \deg h,
\end{aligned}$$

where

$$C_2 := \max\{2 \deg G_1, \deg G_0 + \deg G_1 + \deg A_1, 2 \deg G_0 + \deg A_0\}.$$

We argue similarly for $|S_4|$:

$$\begin{aligned}
|S_4| &\leq |\{\nu \in S_0 : \ \nu(\rho_1) > 0 \text{ or } \nu(\rho_2) > 0\}| + |\{\nu \in S_0 : \ \nu(\rho_1) < 0 \text{ or } \nu(\rho_2) < 0\}| \\
&\leq |\{\nu \in S_0 : \nu(G_1(y)^2 - G_0(y)G_1(y)A_1(y) - A_0(y)G_0(y)^2) > 0\}| \\
&\quad + |\{\nu \in S_0 : \nu(A_1(y)^2 + 4A_0(y)) > 0\}| \\
&\leq \mathcal{H}((G_1^2 - G_0G_1A_1 - G_0^2A_0)(y)) + \mathcal{H}((A_1^2 + 4A_0)(y)) \\
&\leq (C_1 + C_2)\mathcal{H}(y) = (C_1 + C_2)\mathcal{H}(x) < (C_1 + C_2)4 \deg h.
\end{aligned}$$

This gives

$$\begin{aligned}|S| &\le |S_1| + |S_2| + |S_3| + |S_4| + |S_\infty| \\ &< 8 \deg A_0 \deg h + 8 \deg h(C_1 + C_2) + 4 \deg h \\ &= (8(\deg A_0 + C_1 + C_2) + 4) \deg h.\end{aligned}$$

Finally we get

$$\begin{aligned}\mathcal{H}(u_2) &\le 2\mathfrak{g} - 2 + |S| \\ &< 8C_1 \deg h^2 + (8(\deg A_0 + C_1 + C_2) + 4) \deg h - 2 \\ &< (8C_1 + 8(\deg A_0 + C_1 + C_2) + 4) \deg h^2 \\ &= 4(2 \deg A_0 + 4C_1 + 2C_2 + 1) \deg h^2.\end{aligned}$$

We continue to estimate the terms in (19). To give an upper bound on $\mathcal{H}(\alpha_i)$, note that for $\mathcal{H}(\Delta(x)) = \mathcal{H}(\sqrt{\Delta(x)}^2) = 2\mathcal{H}(\sqrt{\Delta(x)})$ it follows that

$$\mathcal{H}(\sqrt{A_1(x)^2 + 4A_0(x)}) = \frac{1}{2}\mathcal{H}(A_1(x)^2 + 4A_0(x)).$$

Therefore, by (21) we get

$$\mathcal{H}(\alpha_i) \le \mathcal{H}(A_1(x)) + \mathcal{H}(\sqrt{A_1(x)^2 + 4A_0(x)}) \le \frac{3}{2}C_1\mathcal{H}(x), \quad i = 1, 2.$$

Using $\mathcal{H}(x) = \mathcal{H}(y)$, we obtain the same upper bound for $\mathcal{H}(\beta_1)$ and $\mathcal{H}(\beta_2)$:

$$\mathcal{H}(\beta_i) \le \frac{3}{2}C_1\mathcal{H}(x), \quad i = 1, 2.$$

Furthermore, we have

$$\begin{aligned}\mathcal{H}(\pi_1) + \mathcal{H}(\pi_2) &= \mathcal{H}\left(\frac{G_1(x) - \alpha_2 G_0(x)}{\alpha_1 - \alpha_2}\right) + \mathcal{H}\left(-\frac{G_1(x) - \alpha_1 G_0(x)}{\alpha_1 - \alpha_2}\right) \\ &\le \mathcal{H}(G_1(x)) + \mathcal{H}(\alpha_2) + \mathcal{H}(G_0(x)) + \mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2) + \\ &\quad + \mathcal{H}(G_1(x)) + \mathcal{H}(\alpha_1) + \mathcal{H}(G_0(x)) + \mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2) \\ &= 2(\mathcal{H}(G_0(x)) + \mathcal{H}(G_1(x))) + 3(\mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2)) \\ &\le (2(\deg G_0 + \deg G_1) + 9C_1)\mathcal{H}(x).\end{aligned}$$

It therefore follows that

$$\mathcal{H}(\alpha_1) + \mathcal{H}(\alpha_2) + \mathcal{H}(\pi_1) + \mathcal{H}(\pi_2) \le (2(\deg G_0 + \deg G_1) + 12C_1)\mathcal{H}(x). \tag{22}$$

Next, we estimate the height of w_2 in a similar way:

$$\begin{aligned}\mathcal{H}(w_2) = \mathcal{H}\left(\frac{\rho_1}{\rho_2}\right) &= \mathcal{H}\left(-\frac{G_1(y) - \beta_2 G_0(y)}{G_1(y) - \beta_1 G_0(y)}\right) \\ &\le 2(\mathcal{H}(G_1(y)) + \mathcal{H}(G_0(y))) + \mathcal{H}(\beta_1) + \mathcal{H}(\beta_2) \\ &\le 2(\deg G_1 + \deg G_0)\mathcal{H}(y) + 3C_1\mathcal{H}(y) \\ &< (2(\deg G_0 + \deg G_1) + 3C_1)4 \deg h \\ &< (2(\deg G_0 + \deg G_1) + 3C_1)4 \deg h^2.\end{aligned}$$

Thus

$$H(u_2) + \mathcal{H}(w_2) < 4 \deg h^2 \left(2(\deg A_0 + \deg G_0 + \deg G_1) + 7C_1 + 2C_2 + 1\right). \tag{23}$$

We now find a lower bound for $\mathcal{H}(v_2)$ in terms of $\mathcal{H}(x)$:

$$\begin{aligned}
\mathcal{H}(v_2) &= \mathcal{H}\left(\frac{\beta_1}{\beta_2}\right) = \mathcal{H}\left(\frac{A_1(y) - \sqrt{A_1(y)^2 + 4A_0(y)}}{A_1(y) + \sqrt{A_1(y)^2 + 4A_0(y)}}\right) \\
&= \mathcal{H}\left(1 - 2 \cdot \frac{\sqrt{A_1(y)^2 + 4A_0(y)}}{A_1(y) + \sqrt{A_1(y)^2 + 4A_0(y)}}\right) \\
&= \mathcal{H}\left(\frac{\sqrt{A_1(y)^2 + 4A_0(y)}}{A_1(y) + \sqrt{A_1(y)^2 + 4A_0(y)}}\right) = \mathcal{H}\left(\frac{A_1(y)}{\sqrt{A_1(y)^2 + 4A_0(y)}} + 1\right) \\
&= \mathcal{H}\left(\sqrt{\frac{A_1(y)^2}{A_1(y)^2 + 4A_0(y)}}\right) = \frac{1}{2}\mathcal{H}\left(\frac{A_1(y)^2 + 4A_0(y)}{A_1(y)^2}\right) \\
&= \frac{1}{2}\mathcal{H}\left(\frac{A_0(y)}{A_1(y)^2}\right).
\end{aligned}$$

Note that

$$\mathcal{H}\left(\frac{A_0(y)}{A_1(y)^2}\right) \geq |\mathcal{H}(A_0(y)) - \mathcal{H}(A_1(y)^2)| = |\deg A_0 - 2\deg A_1| \cdot \mathcal{H}(y).$$

If $\deg A_0 \neq 2 \deg A_1$, then clearly

$$\mathcal{H}\left(\frac{A_0(y)}{A_1(y)^2}\right) \geq \mathcal{H}(y).$$

If on the other hand we have that $\deg A_0 = 2 \deg A_1$, then by the polynomial remainder theorem we have that $A_0(y) = A_1(y)^2 q(y) + r(y)$, where $q \in \mathbb{C}$ is constant and $\deg r < 2 \cdot \deg A_1$. Thus,

$$\begin{aligned}
\mathcal{H}\left(\frac{A_0(y)}{A_1(y)^2}\right) &= \mathcal{H}\left(q(y) + \frac{r(y)}{A_1(y)^2}\right) = \mathcal{H}\left(\frac{r(y)}{A_1(y)^2}\right) \\
&\geq \mathcal{H}(A_1(y)^2) - \mathcal{H}(r(y)) = (2\deg A_1 - \deg r) \cdot \mathcal{H}(y) \geq \mathcal{H}(y).
\end{aligned}$$

Thus,

$$\mathcal{H}(v_2)) \geq \frac{1}{2}\mathcal{H}(y) = \frac{1}{2}\mathcal{H}(x). \tag{24}$$

(Note that since $\mathcal{H}(v_2) \neq 0$, we cannot have $\deg A_0 = \deg A_1 = 0$).

Considering again (19), by (22), (23) and (24) we find that

$$\mathcal{H}(G_n(x)) < C \deg h^2,$$

where $C = 16\left(2(\deg A_0 + \deg G_0 + \deg G_1) + 7C_1 + 2C_2 + 1\right)(\deg G_0 + \deg G_1 + 6C_1)$.

To give a suitable lower bound for $\mathcal{H}(G_n(x))$, note that since $G_n = g \circ h$ we have

$$\mathcal{H}(G_n(x)) = \deg g \deg h \cdot [F : \mathbb{C}(x)] = \deg g \deg h \cdot [F : \mathbb{C}(x, y)] \cdot [\mathbb{C}(x, y) : \mathbb{C}(x)].$$

By Lemma 3 it follows that $[\mathbb{C}(x, y) : \mathbb{C}(x)] \geq \frac{1}{2} \deg h$. Therefore, we have

$$\mathcal{H}(G_n(x)) \geq \frac{1}{2} \deg g \deg h^2 \cdot [F : \mathbb{C}(x, y)] \geq \frac{1}{2} \deg g \deg h^2.$$

Finally, we conclude that

$$\frac{1}{2} \deg g \deg h^2 \leq \mathcal{H}(G_n(x)) < C \deg h^2,$$

and therefore that $\deg g < 2C$. □

Acknowledgements. Open access funding provided by Austrian Science Fund (FWF). The work on this manuscript was supported by FWF (Austrian Science Fund) Grant No. P24574 and No. J3955.

References

[1] Beals, R.M., Wetherell, J.L., Zieve, M.E.: Polynomials with a common composite. Isr. J. Math. **174**, 93–117 (2009)
[2] Beardon, A.F., Ng, T.W.: On Ritt's factorization of polynomials. J. London. Math. Soc. **62**, 127–138 (2000)
[3] Bilu, Yu.F.: Quadratic factors of $f(x) - g(y)$. Acta Arith. **90**, 341–355 (1999)
[4] Bilu, Yu.F., Tichy, R.F.: The Diophantine equation $f(x) = g(y)$. Acta Arith. **95**, 261–288 (2000)
[5] Brownawell, W.D., Masser, D.W.: Vanishing sums in function fields. Math. Proc. Cambridge Philos. Soc. **100**(3), 427–434 (1986)
[6] Dujella, A., Tichy, R.F.: Diophantine equations for second-order recursive sequences of polynomials. Q. J. Math. **52**, 161–169 (2001)
[7] Fried, M.D.: On a conjecture of Schur. Michigan Math. J. **17**, 41–55 (1970)
[8] Fuchs, C.: On the Diophantine equation $G_n(x) = G_m(P(x))$ for third order linear recurring sequences. Port. Math. (N.S.) **61**, 1–24 (2004)
[9] Fuchs, C., Pethő, A.: Effective bounds for the zeros of linear recurrences in function fields. J. Theor. Nombres Bordeaux **17**(3), 749–766 (2005)
[10] Fuchs, C., Pethő, A., Tichy, R.F.: On the Diophantine equation $G_n(x) = G_m(P(x))$. Monatsh. Math. **137**, 173–196 (2002)
[11] Fuchs, C., Pethő, A., Tichy, R.F.: On the equation $G_n(x) = G_m(P(x))$: Higher order recurrences. Trans. Am. Math. Soc. **355**, 4657–4681 (2003)

[12] Fuchs, C., Pethő, A., Tichy, R.F.: On the Diophantine equation $G_n(x) = G_m(y)$ with $Q(x, y) = 0$. Dev. Math. **16**, 199–209. In: Diophantine Approximation Festschrift for Wolfgang Schmidt. (H.P. Schlickewei, K. Schmidt, R.F. Tichy, eds.), Springer-Verlag, Vienna, (2008)
[13] Fuchs, C., Zannier, U.: Composite rational functions expressible with few terms. J. Eur. Math. Soc. (JEMS) **14**, 175–208 (2012)
[14] Kirschenhofer, P., Pfeiffer, O.: Diophantine equations between polynomials obeying second order recurrences. Period. Math. Hungar. **47**, 119–134 (2003). https://doi.org/10.1023/B:MAHU.0000010816.85657.40
[15] Kreso, D.: Diophantine equations in separated variables and lacunary polynomials. Int. J. Number Theory **13**, 2055–2074 (2017)
[16] Kreso, D.: On common values of lacunary polynomials at integer points. N. Y. J. Math. **21**, 987–1001 (2015)
[17] Kreso, D., Zieve, M.E.: On factorizations of maps between curves. arXiv:1405.4753
[18] Mason, R.C.: Diophantine Equations Over Function Fields. Cambridge University Press, Cambridge (1984)
[19] Müller, P.: Permutation Groups with a cyclic Two-Orbits Subgroup and Monodromy Groups of Siegel Functions, arXiv:math/0110060
[20] Müller, P., Zieve, M.E.: On Ritt's polynomial decomposition theorems. arXiv:0807.3578
[21] Ritt, J.F.: Prime and composite polynomials. Trans. Am. Math. Soc. **23**, 51–66 (1922)
[22] Schinzel, A.: Polynomials with Special Regard to Reducibility. Cambridge University Press, Cambridge (2000)
[23] Stichtenoth, H.: Function Fields and Codes. Universitext, Springer, Berlin (1993)
[24] Turnwald, G.: On Schur's conjecture. J. Austral. Math. Soc. Ser. A **58**, 312–357 (1995)
[25] Zannier, U.: On the integer solutions of exponential equations in function fields. Ann. Inst. Fourier (Grenoble) **54**(4), 849–874 (2004)
[26] Zannier, U.: On the number of terms of a composite polynomial. Acta Arith. **127**(2), 157–167 (2007)
[27] Zannier, U.: On composite lacunary polynomials and the proof of a conjecture of Schinzel. Invent. Math. **174**, 127–138 (2008)